CLAIMS:

1. A method of establishing a secure authenticated channel between two devices device A and device B, where A authenticates to B using challenge/response public key cryptography, and device B authenticates to device A using a zero-knowledge protocol.

2. The method of claim 1, in which the zero-knowledge protocol is a Guillou-Quisquater zero-knowledge protocol.

3. The method of claim 1, in which the zero-knowledge protocol is a Fiat-Shamir zero-knowledge protocol.

4. The method of claim 1, in which the zero-knowledge protocol is a Schnorr zero-knowledge protocol.

5. The method of claim 1, in which device B authenticates to device A using a combination of the zero-knowledge protocol and a broadcast-encryption system, where a secret used in the zero-knowledge protocol is scrambled such that it can only be obtained by those that can process a broadcast encryption key-block successfully.

6. The method of claim 5, where the secret used in the zero-knowledge protocol is encrypted by the root-key K_{root} of a broadcast encryption system key-block.

7. The method of claim 5, where there is one key block with a root key $K_{root,1}$ to allow for authentication, and another key block with root key $K_{root,2}$ for content encryption.

8. The method of claim 1 or 5, where the zero-knowledge pair {J,s} is different for every key-block.

9. The method of claim 1 or 5, in which device B generates a bas key and sends the bas key to device A.

10. The method of claim 9 as dependent from 5, in which device A only accepts the bas key if device A can verify that device B can descramble the secret.

11. A system comprising a first device A and a second device B, where the device A is arranged to authenticate to the device B using challenge/response public key cryptography, and the device B is arranged to authenticate to the device A using a zero-knowledge protocol.

12. A first device A arranged to authenticate itself to a second device B using challenge/response public key cryptography, and arranged to authenticate the second device B using a zero-knowledge protocol.

13. A second device B arranged to authenticate itself to a first device A using a zero-knowledge protocol, and arranged to authenticate the first device A using challenge/response public key cryptography.

14. A computer program product comprising code enabling a programmable device to operate as the first device of claim 12 and/or the second device of claim 13.